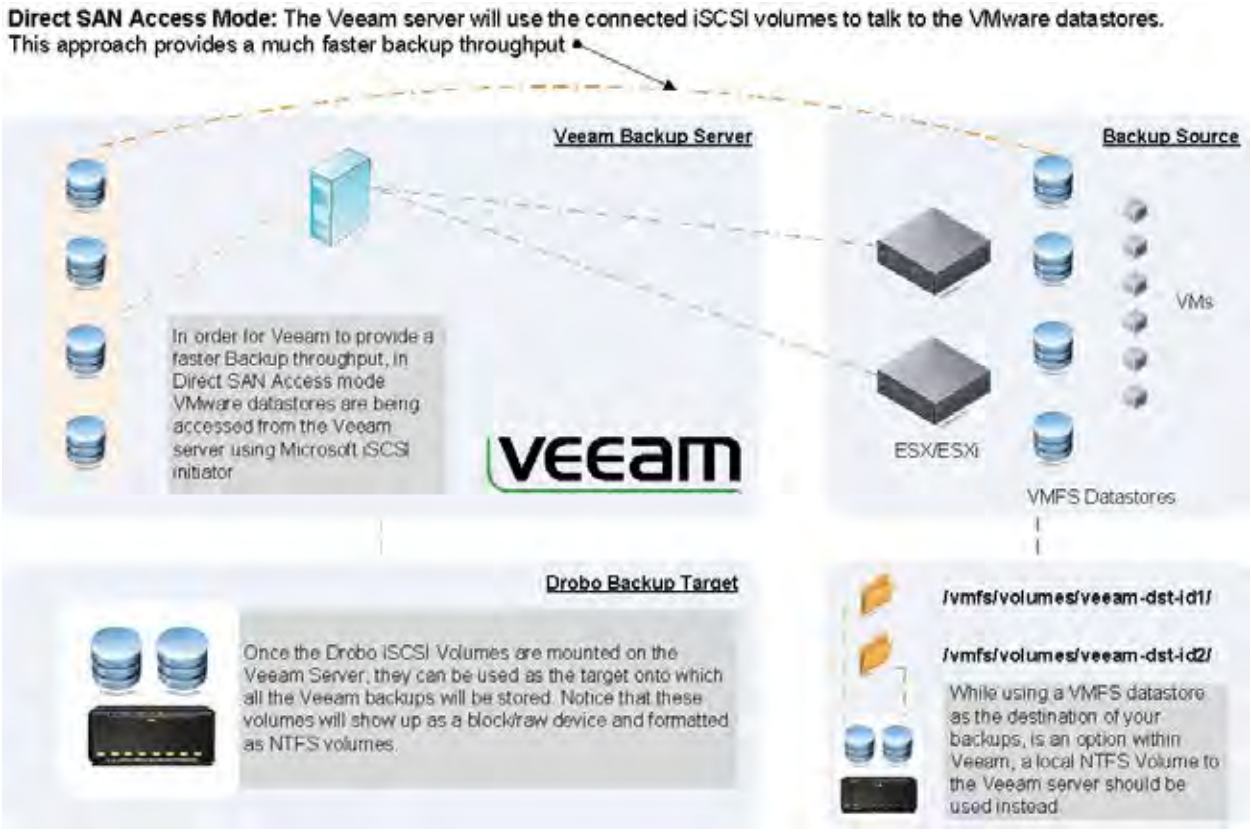
This document shows you how to use a Drobo iSCSI array with Veeam Backup & Replication version 5 in a VMware environment. Veeam provides fast disk-based backup and recovery of virtual machines (VMs), while Drobo provides an easy-to-use and scalable disk-based storage target. The combined solution provides reliable and affordable disk-based backup storage for your virtualized server environment. The benefit of this solution is the ability to have many different restore points on disk media instead of tape for faster backups and restores without the hassle of managing catalogs of tapes.

Topics

- Veeam basics
- Creating and mounting a Drobo volume
- Using Microsoft iSCSI Initiator to connect to VMware datastores
- Adding a new vCenter Server
- Creating a new Veeam Backup job
- Restoring virtual machines with Veeam Backup


Direct SAN Access Mode: The Veeam server will use the connected iSCSI volumes to talk to the VMware datastores. This approach provides a much faster backup throughput
Veeam Backup Server
Backup Source
VMs
ESX/ESXi
VMFS Datastores
In order for Veeam to provide a faster Backup throughput, in Direct SAN Access mode VMware datastores are being accessed from the Veeam server using Microsoft iSCSI initiator
VEEAM
Drobo Backup Target
Once the Drobo iSCSI Volumes are mounted on the Veeam Server, they can be used as the target onto which all the Veeam backups will be stored. Notice that these volumes will show up as a block/raw device and formatted as NTFS volumes.
/vmfs/volumes/veeam-dst-id1/
/vmfs/volumes/veeam-dst-id2/
While using a VMFS datastore as the destination of your backups, is an option within Veeam, a local NTFS Volume to the Veeam server should be used instead.

What You Will Need

- Drobo model B800i or B1200i
- Drobo Dashboard management software (most recent version)
- Enterprise-grade 7200RPM SAS or SATA disk drives (recommended)
- Windows Server 2008 R2 (dedicated server recommended)
- Veeam Backup and Replication version 5

Veeam Basics

Veeam can be installed on a physical or virtual server. The advantage of installing on a physical server is that backup storage can be directly attached and deliver the best throughput as well as attaching a tape library to the same physical server should this is still required in addition to disk-based backup. Further, installing Veeam as a physical server offloads the CPU burden of the backups from the VMware cluster.

Veeam Backup & Replication version 5 provides:

- File-level recovery
- Start virtual machine from the backup
- Provide replication
- Built in deduplication and compression
- Allow users to restores their own files
- Backup recovery verification

Backup Modes

Veeam Backup & Replication supports different backup methods depending on the environment. Because Veeam takes advantage of VMware Storage APIs, Direct SAN Access is preferred because it's the most efficient method and will be used in this document. Three transport modes are available:

- *Direct SAN Access.* Supported only for VMs that reside on a block storage device (iSCSI). In Direct SAN Access mode, Veeam runs on a physical server and backs up the VM datastores directly without going through the ESX/ESXi host. Direct SAN Access mode also adds failover safety mechanisms. Note that if Direct SAN Access mode becomes unavailable, Veeam fails over to Network mode in order to complete the backup.
- *Virtual Appliance.* In this mode Veeam is installed on a VM and disks from the VMs that are to be backed up are "hot-added" to the Veeam VM. Data is read directly from the storage stack instead of over the network. The advantage of using Virtual Appliance mode is its ability to directly back up VMs on NFS storage.
- *Network* The least efficient mode because the Veeam Backup & Replication server is connected to the ESX/ESXi host over the network using Network Block Device Protocol (NBD) to connect to the VM datastore. This adds additional network traffic and resource usage on the host, which can negatively impact VMs running on the host.

Veeam Hardware Requirements

Veeam recommends dedicating a server to be used solely for Veeam backups. While a VM host can be the backup server, a physical host would tend to outperform a virtual host, because resources are not shared

and there is no virtualization layer. Make the decision based on the amount of data to be backed up and features you might want to use in Veeam (for example, compression and deduplication).

Network Considerations

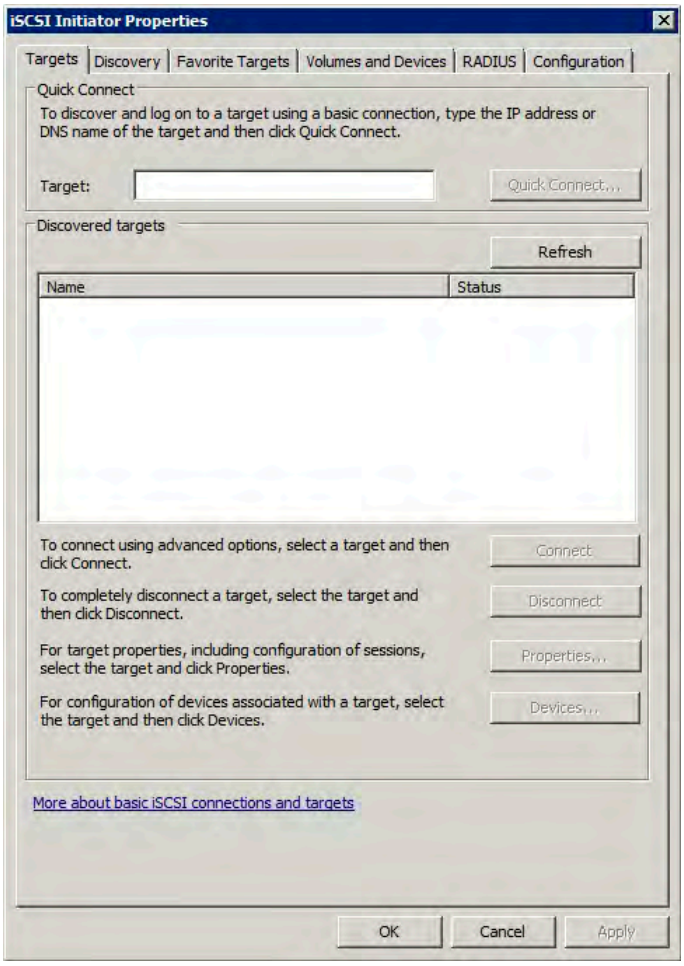
For Network mode backup and restore, Veeam uses the LAN to receive and send data. Therefore, as a best practice, most IT administrators deploy two network interfaces. One interface is used for management (RDP to the server, AD traffic, DNS, and so on). The second interface is dedicated to backup and restore traffic. This results in the best possible backup and restore performance, as it will not overload the management network.

Creating and Mounting a Drobo Volume

Follow the directions in the Drobo Online User Guide to configure the Drobo and create an NTFS volume: http://www.drobo.com/support/documentation.php

STEP 1

In this step, two Drobo volumes are created using Drobo Dashboard. Do NOT install Drobo Dashboard on the Veeam server but on a different host. Once the volume is created, it will be the repository in which Veeam stores its backups.

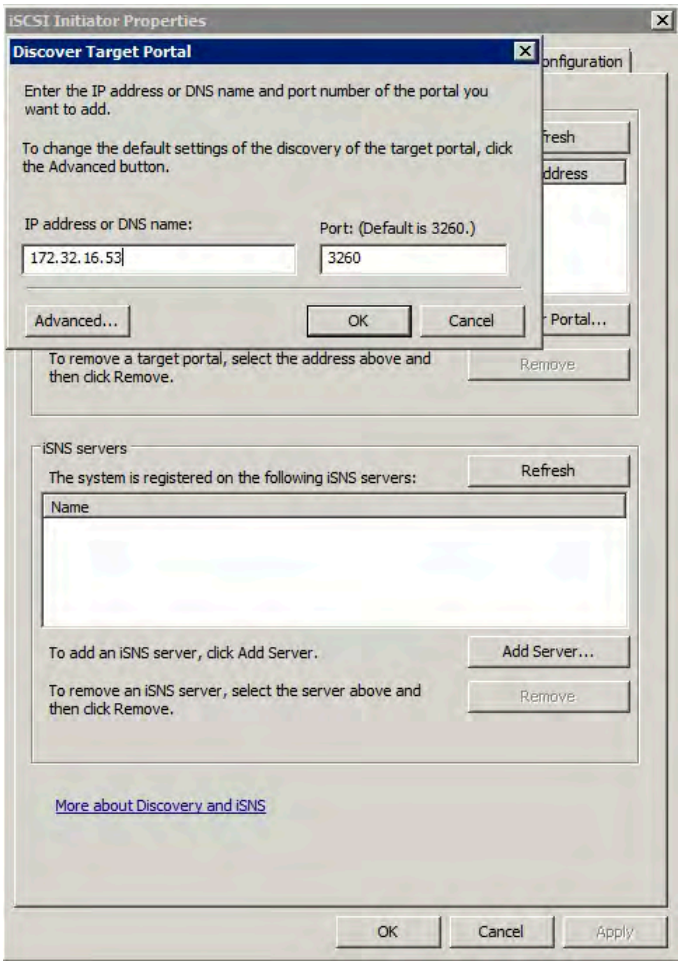

iSCSI Initiator Properties
Targets
Discovery
Favorite Targets
Volumes and Devices
RADIUS
Configuration
Quick Connect
To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.
Target:
Quick Connect...
Discovered targets
Refresh
Name
Status
To connect using advanced options, select a target and then click Connect.
Connect
To completely disconnect a target, select the target and then click Disconnect.
Disconnect
For target properties, including configuration of sessions, select the target and click Properties.
Properties...
For configuration of devices associated with a target, select the target and then click Devices.
Devices...
More about basic iSCSI connections and targets
OK
Cancel
Apply

Mount these volumes using Microsoft iSCSI Initiator on the Veeam server. Once the volumes have been created, using Drobo Dashboard to open Microsoft iSCSI Initiator on the Veeam server: **Start > Administrative Tools > iSCSI Initiator**

If you have not used Microsoft iSCSI Initiator before, you will notice that the list of volumes is empty.

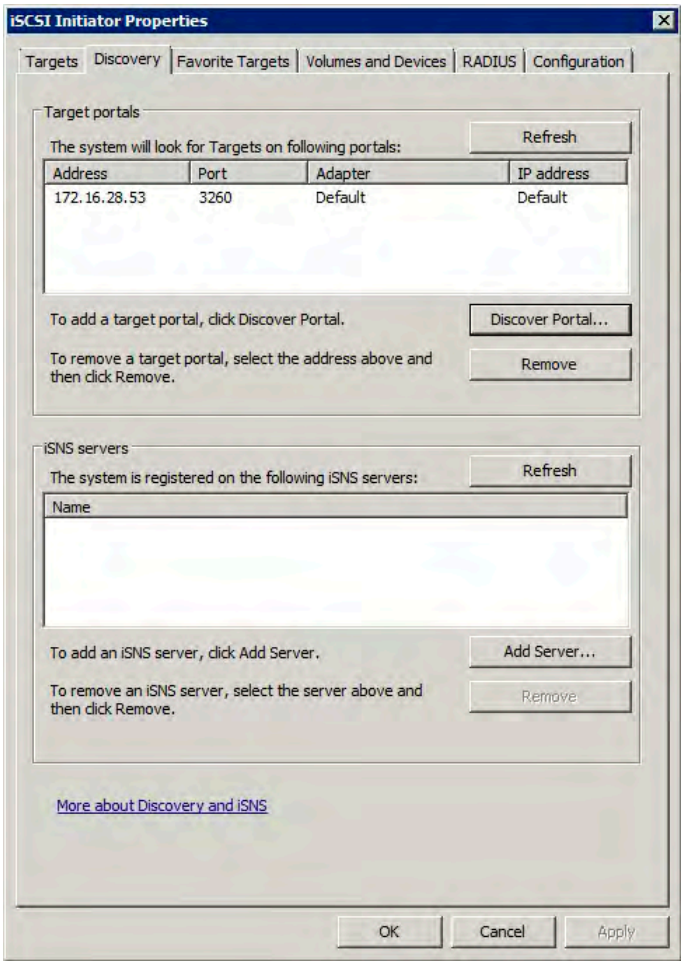
Click the **Discovery** tab.

STEP 2


iSCSI Initiator Properties
Discover Target Portal
Enter the IP address or DNS name and port number of the portal you want to add.
To change the default settings of the discovery of the target portal, click the Advanced button.
IP address or DNS name:
Port: (Default is 3260.)
172.32.16.53
3260
Advanced...
OK
Cancel
To remove a target portal, select the address above and then click Remove.
Remove
iSNS servers
The system is registered on the following iSNS servers:
Refresh
Name
To add an iSNS server, click Add Server.
Add Server...
To remove an iSNS server, select the server above and then click Remove.
Remove
More about Discovery and iSNS
OK
Cancel
Apply

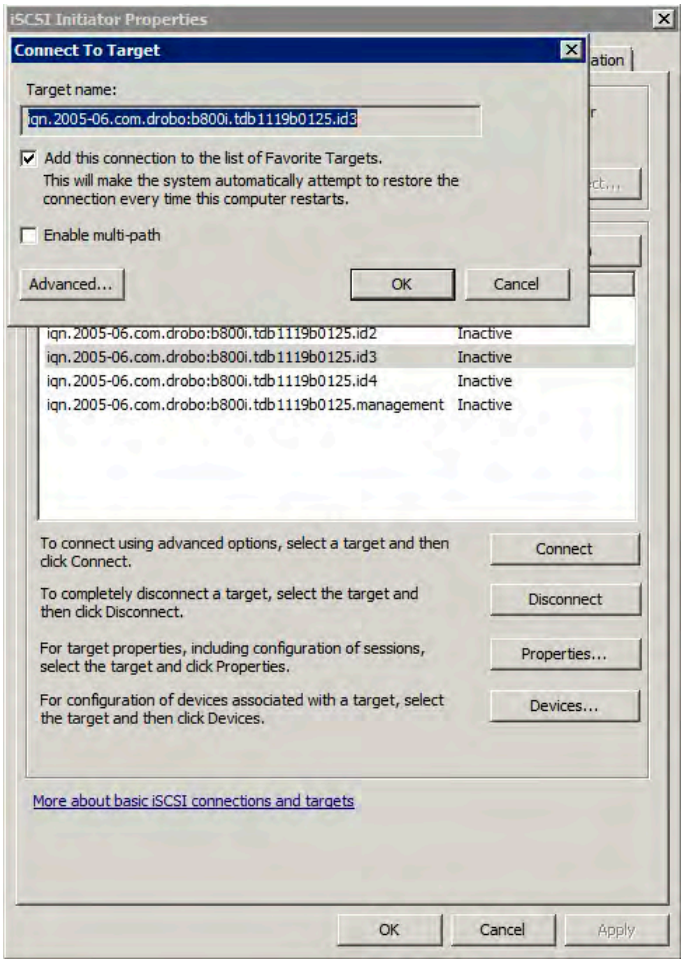
Click the **Discover Portal** button, add the IP address of the Drobo, and click **OK**.

STEP 3



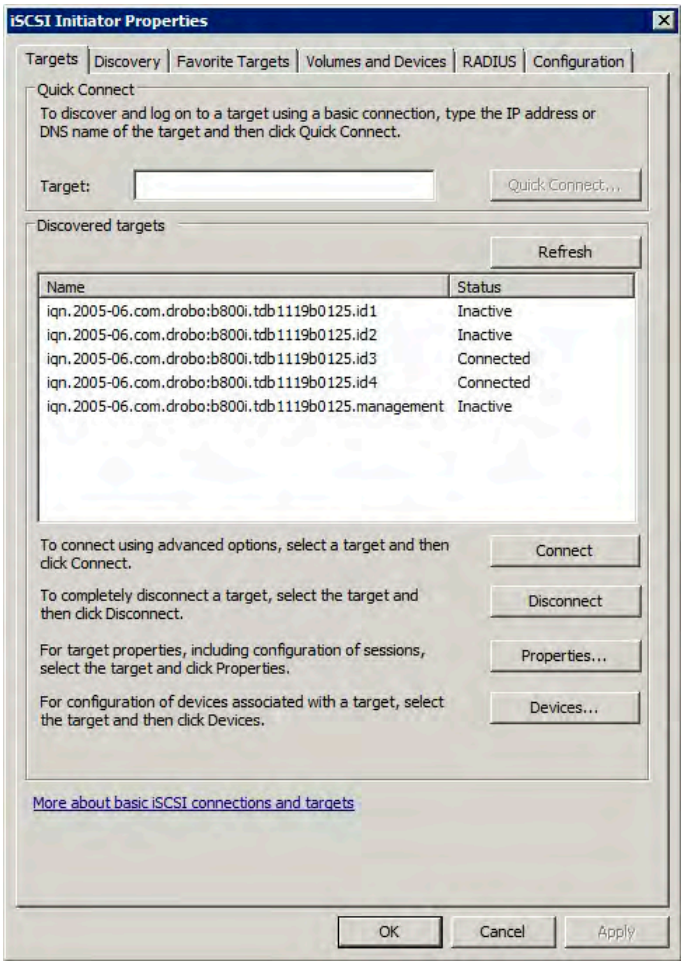
The address is now added in the Target portals list. Click the **Targets** tab.

STEP 4


iSCSI Initiator Properties
Connect To Target
Target name:
iqn.2005-06.com.drobo:b800i.tdb1119b0125.id3
Add this connection to the list of Favorite Targets.
This will make the system automatically attempt to restore the connection every time this computer restarts.
Enable multi-path
Advanced...
OK
Cancel
iqn.2005-06.com.drobo:b800i.tdb1119b0125.id2 Inactive
iqn.2005-06.com.drobo:b800i.tdb1119b0125.id3 Inactive
iqn.2005-06.com.drobo:b800i.tdb1119b0125.id4 Inactive
iqn.2005-06.com.drobo:b800i.tdb1119b0125.management Inactive
To connect using advanced options, select a target and then click Connect.
Connect
To completely disconnect a target, select the target and then click Disconnect.
Disconnect
For target properties, including configuration of sessions, select the target and click Properties.
Properties...
For configuration of devices associated with a target, select the target and then click Devices.
Devices...
More about basic iSCSI connections and targets
OK
Cancel
Apply

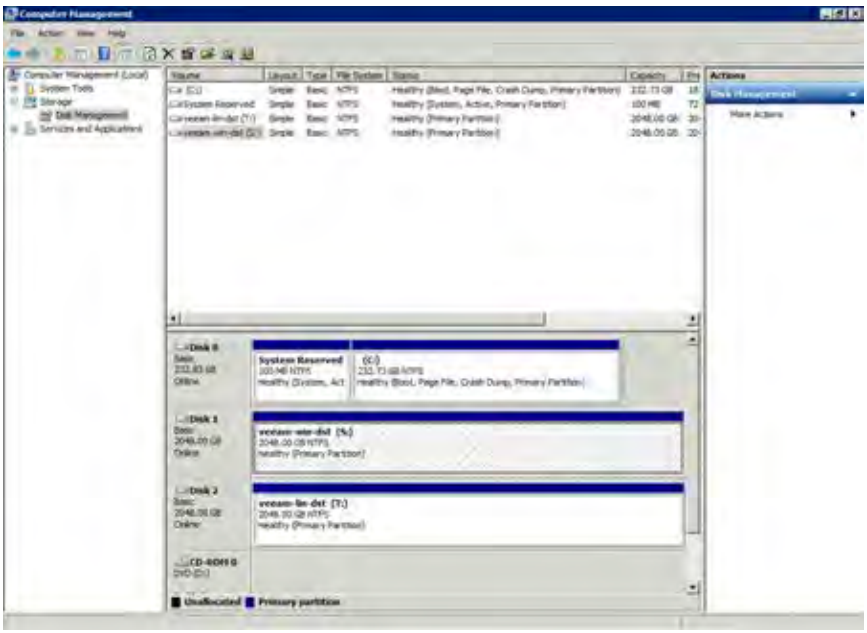
Select the volume you wish to mount, click **Connect**. In the pop-up dialog, and click **OK**.

STEP 5



Once you have selected and connected the volumes you want to use, click **OK** to close Microsoft iSCSI Initiator.

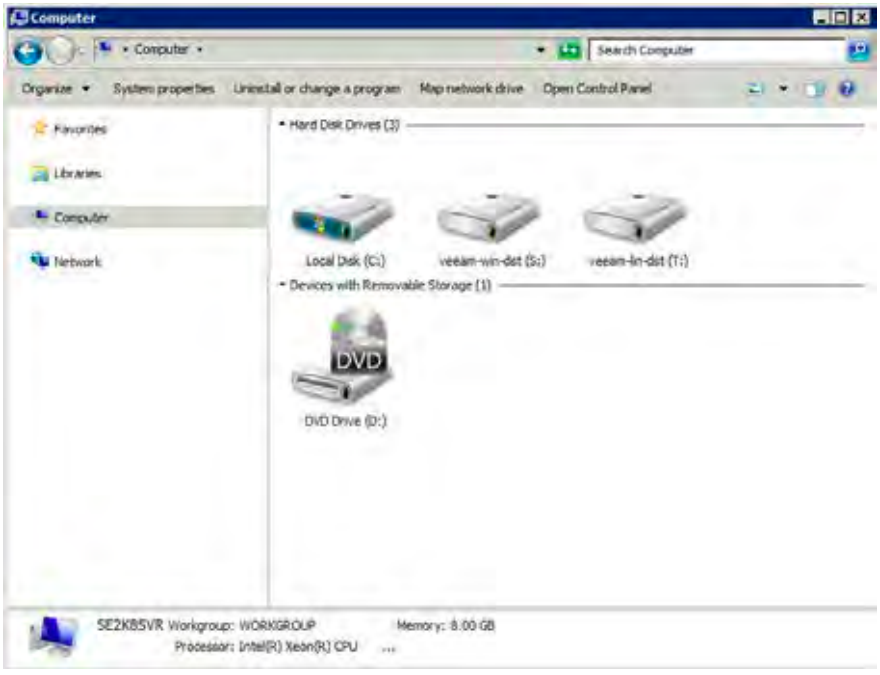
STEP 6



To open Computer Management, choose **Start > Administrative Tools > Computer Management.**

Go to the Disk Management section under Storage. You will now see two additional disks, which are the iSCSI volumes you have just connected to. If the volumes are not mounted, mount them and assign them a drive letter.

STEP 7



A window prompts you to select a folder. In this example, a folder that resides on one of the Drobo volumes is selected.

To learn about Drobo and iSCSI, visit: http://www.drobo.com/resources/iscsi.php

NOTE: Veeam requires Microsoft Windows diskpart automount feature to be *disabled* when the backup mode is Direct SAN Access. However, Drobo Dashboard requires that this feature be *enabled*, so that volumes can be created, mounted, and formatted in Drobo Dashboard. Therefore it is recommended that Drobo Dashboard be installed on a host that is not the Veeam server.

Using Microsoft iSCSI Initiator To Connect to VMware Datastores

As discussed previously, Microsoft iSCSI Initiator is used on the host where Veeam is installed to allow Veeam to:

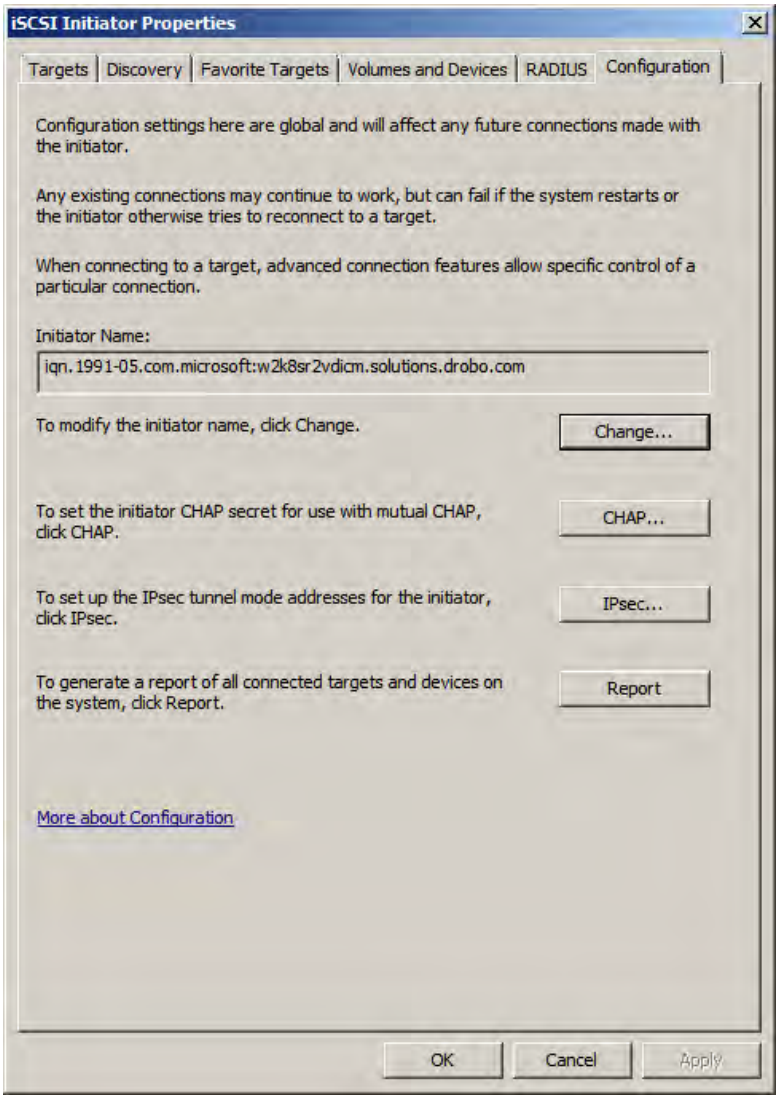
- Connect but NOT mount the ESX/ESXi datastores on which the VMs reside
- Connect but NOT mount the ESX/ESXi datastores to which VMs can be backed up

NOTE: This step is very similar to the previous section, in which Microsoft iSCSI Initiator was used to connect to iSCSI volumes. However, because these volumes are formatted as VMFS, Windows does not show them in My Computer. They do, however, appear as volumes in Disk Management.

There is a potential risk that the VMFS volumes are re-signatured by Windows if you attempt to initialize one of these volumes and or assign it a drive letter. To prevent this from happening, Veeam recommends that the diskpart automount be disabled. This is not applicable if you are using Veeam Backup & Replication version 5, since it will automatically disable automount.

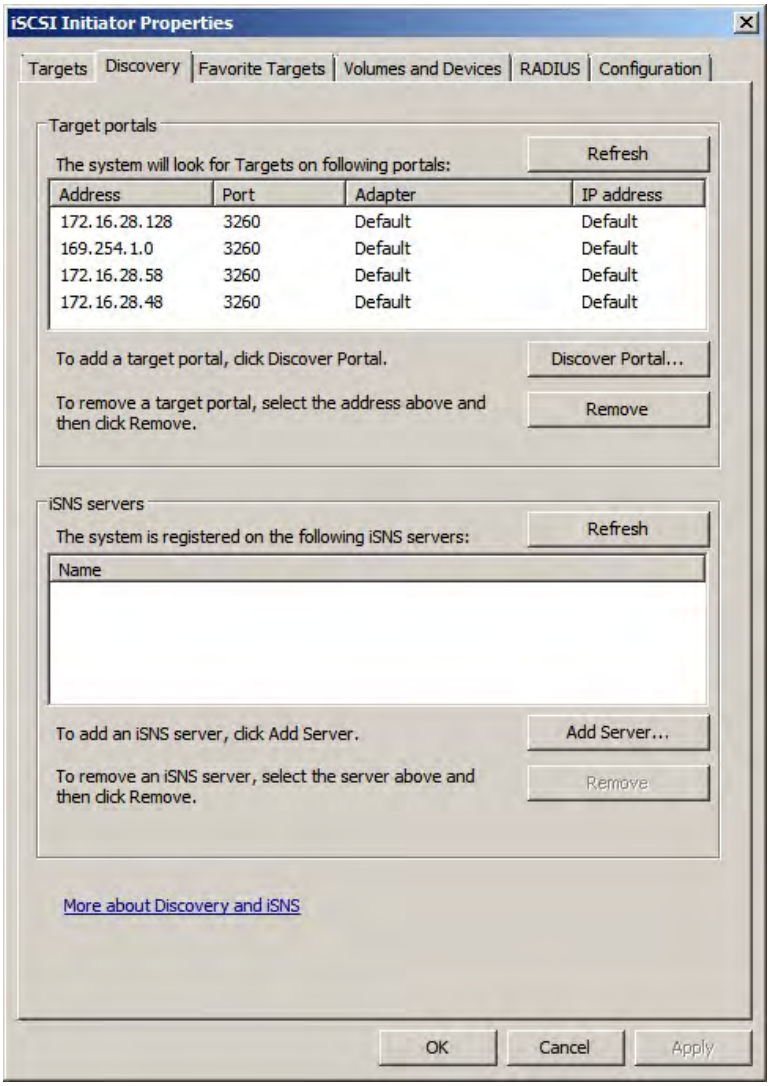
For more information, visit:
http://www.veeam.com/blog/using-the-iscsi-initiator-within-veeam-backup-replication-in-a-vm.html

STEP 1


iSCSI Initiator Properties
Targets
Discovery
Favorite Targets
Volumes and Devices
RADIUS
Configuration
Configuration settings here are global and will affect any future connections made with the initiator.
Any existing connections may continue to work, but can fail if the system restarts or the initiator otherwise tries to reconnect to a target.
When connecting to a target, advanced connection features allow specific control of a particular connection.
Initiator Name:
iqn.1991-05.com.microsoft:w2k8sr2vdicm.solutions.drobo.com
To modify the initiator name, click Change.
Change...
To set the initiator CHAP secret for use with mutual CHAP, click CHAP.
CHAP...
To set up the IPsec tunnel mode addresses for the initiator, click IPsec.
IPsec...
To generate a report of all connected targets and devices on the system, click Report.
Report
More about Configuration
OK
Cancel
Apply

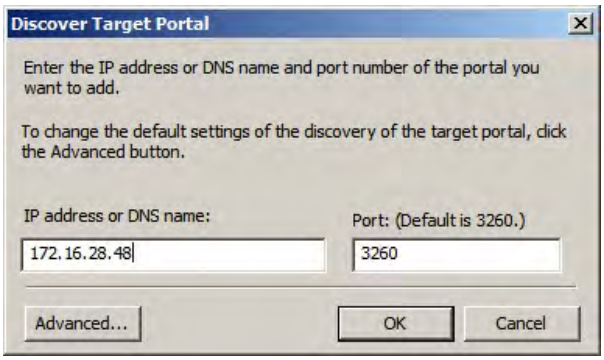
To open Microsoft iSCSI Initiator, choose **Start > Administrative Tools > iSCSI Initiator**.

STEP 2



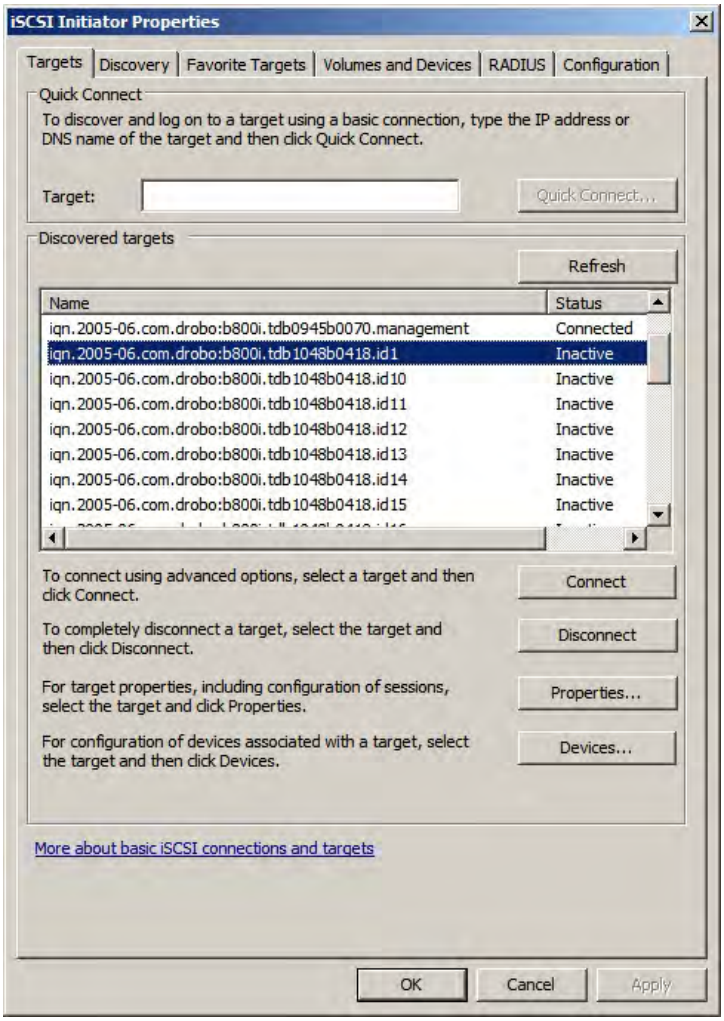
In the Discovery tab, click **Discover Portal**.

STEP 3


Discover Target Portal
Enter the IP address or DNS name and port number of the portal you want to add.
To change the default settings of the discovery of the target portal, click the Advanced button.
IP address or DNS name:
Port: (Default is 3260.)
172.16.28.48
3260
Advanced...
OK
Cancel

Enter the IP address of the array. Shortly thereafter a list of all the volumes that your backup server has access to appears the Targets tab.

STEP 4

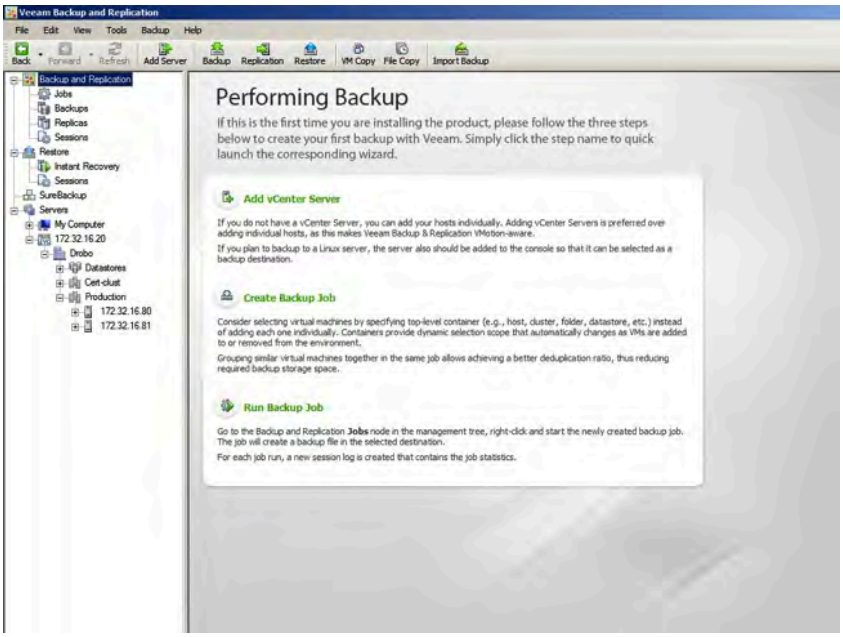


Select each target that you want to mount and click **Connect**.

Adding a New vCenter Server

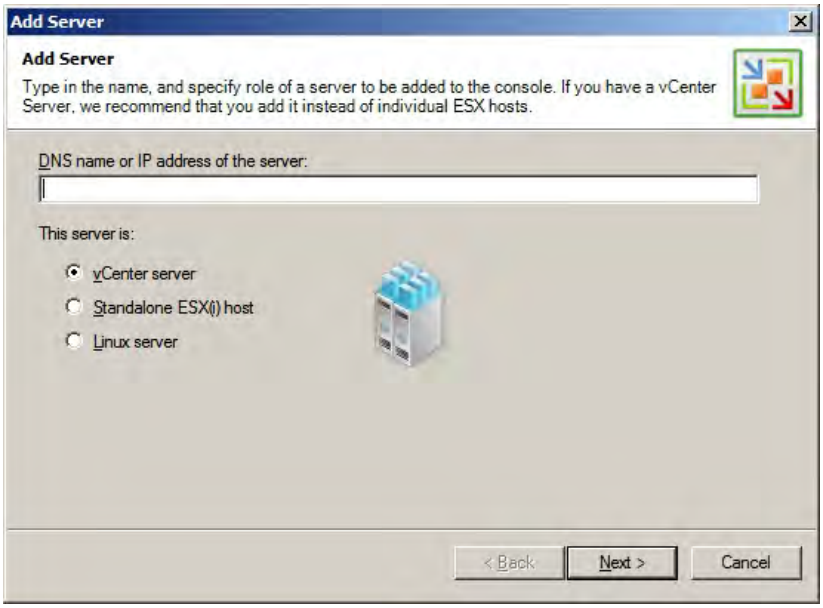
Install Veeam and use the main console to configure and manage backup attributes such as schedules, retention, targets, deduplication, compression, and so on.

STEP 1


Veeam Backup and Replication
File Edit View Tools Backup Help
Back Forward Refresh Add Server Backup Replication Restore VM Copy File Copy Import Backup
Backup and Replication
Jobs
Backups
Replicas
Sessions
Restore
Instant Recovery
Sessions
SureBackup
Servers
My Computer
172.32.16.20
Drobo
Datastores
Cert-clust
Production
172.32.16.80
172.32.16.81
Performing Backup
If this is the first time you are installing the product, please follow the three steps below to create your first backup with Veeam. Simply click the step name to quick launch the corresponding wizard.
Add vCenter Server
If you do not have a vCenter Server, you can add your hosts individually. Adding vCenter Servers is preferred over adding individual hosts, as this makes Veeam Backup & Replication vMotion-aware.
If you plan to backup to a Linux server, the server also should be added to the console so that it can be selected as a backup destination.
Create Backup Job
Consider selecting virtual machines by specifying top-level container (e.g., host, cluster, folder, datastore, etc.) instead of adding each one individually. Containers provide dynamic selection scope that automatically changes as VMs are added to or removed from the environment.
Grouping similar virtual machines together in the same job allows achieving a better deduplication ratio, thus reducing required backup storage space.
Run Backup Job
Go to the Backup and Replication Jobs node in the management tree, right-click and start the newly created backup job. The job will create a backup file in the selected destination.
For each job run, a new session log is created that contains the job statistics.

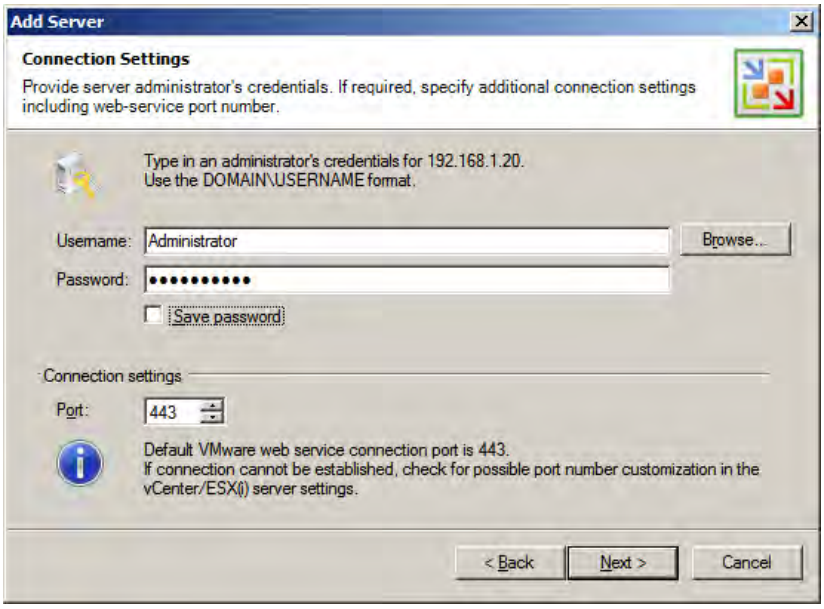
Launch Veeam and click **Add vCenter Server**.

STEP 2


Add Server
Add Server
Type in the name, and specify role of a server to be added to the console. If you have a vCenter Server, we recommend that you add it instead of individual ESX hosts.
DNS name or IP address of the server:
This server is:
vCenter server
Standalone ESX(i) host
Linux server
< Back
Next >
Cancel

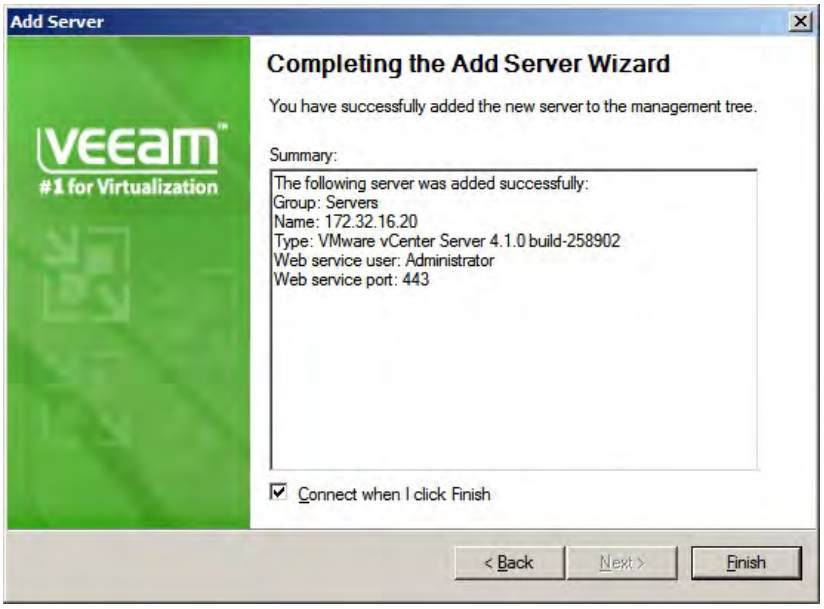
Enter the IP address of the server, whether you are adding a vCenter server or a single ESX/ESXi host.

STEP 3


Add Server
Connection Settings
Provide server administrator's credentials. If required, specify additional connection settings including web-service port number.
Type in an administrator's credentials for 192.168.1.20.
Use the DOMAIN\USERNAME format.
Username:
Administrator
Browse...
Password:
Save password
Connection settings
Port:
443
Default VMware web service connection port is 443.
If connection cannot be established, check for possible port number customization in the vCenter/ESX(i) server settings.
< Back
Next >
Cancel

Provide server administrator credentials.

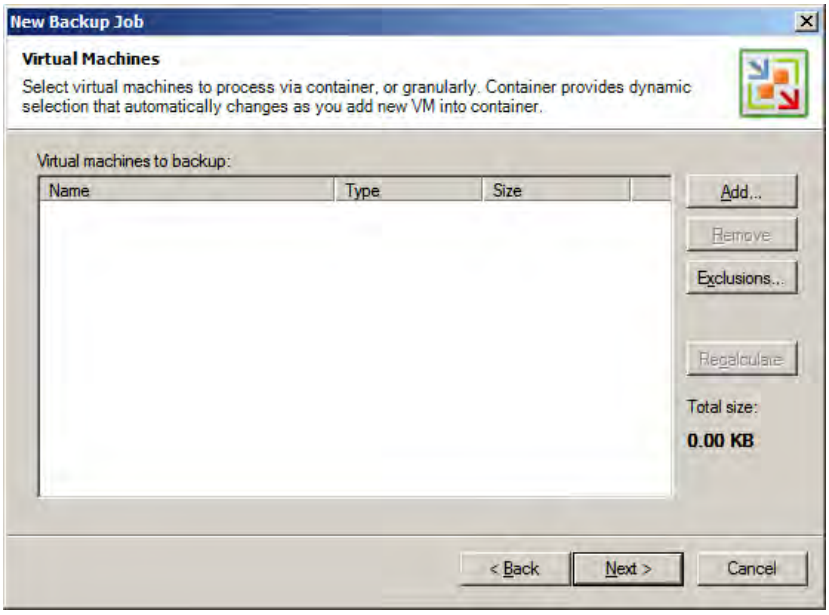
STEP 4



Click **Finish** to complete the Add Server wizard.

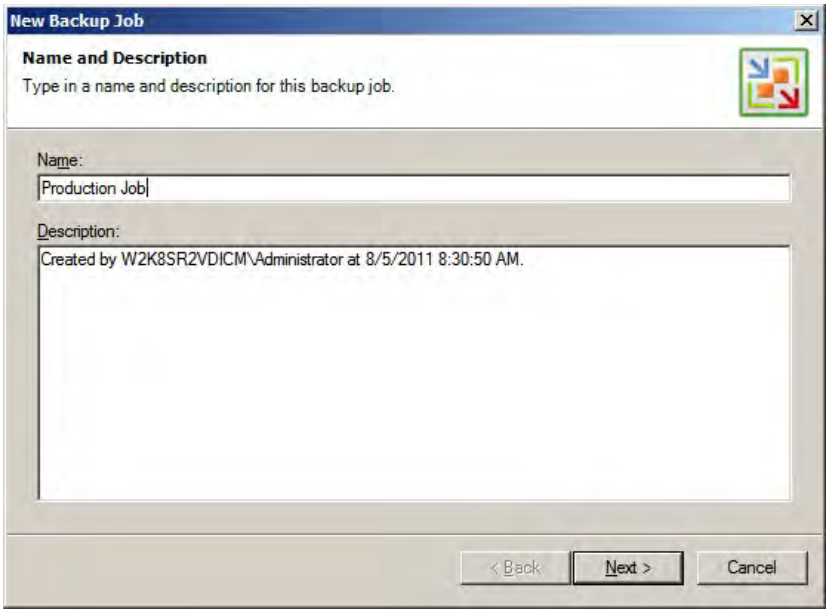
Creating a New Veeam Backup Job

STEP 1



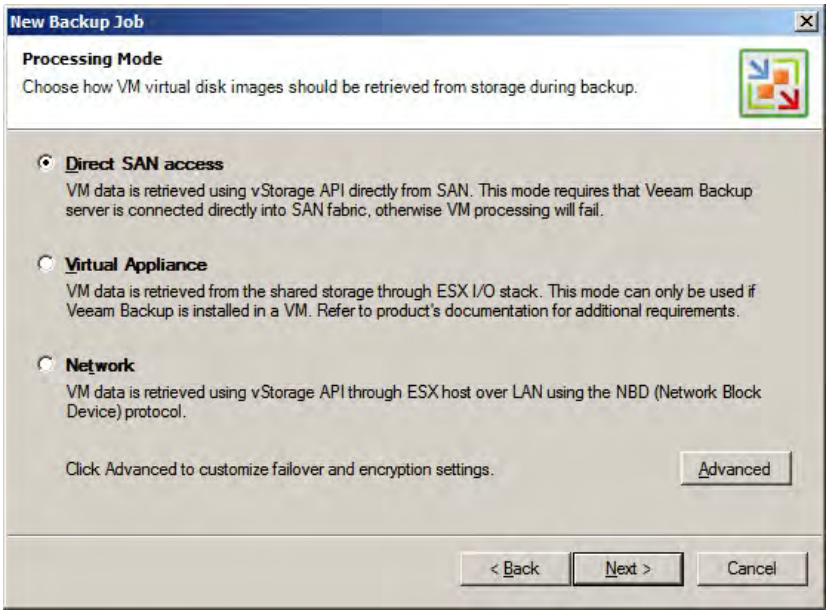
Click **Create Backup Job** and click **Add**.

STEP 2



Enter a name for the backup job. In this example, the name is Production Job.

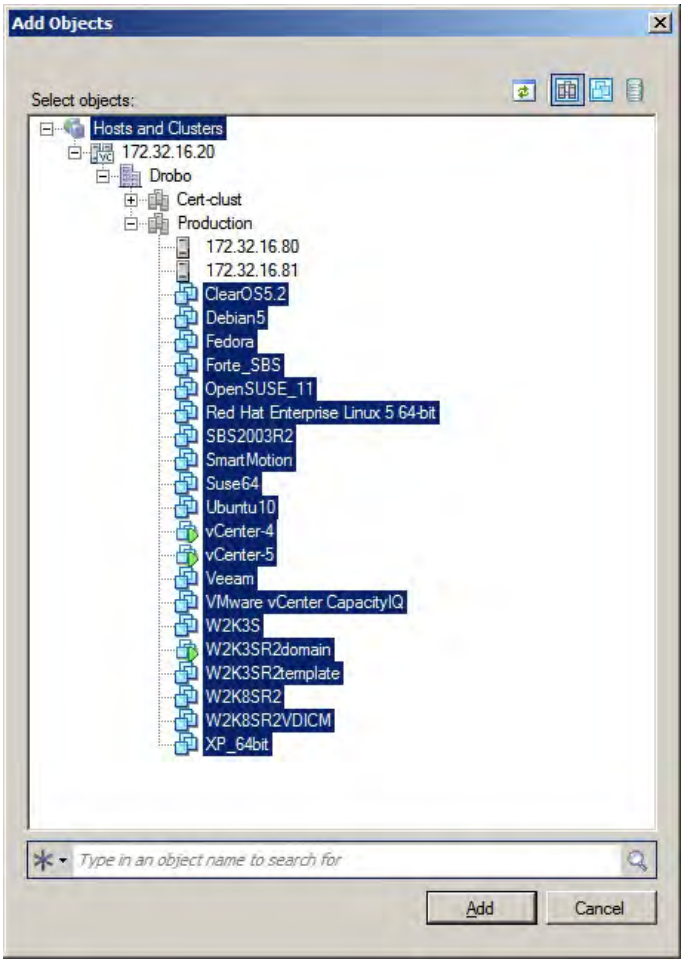
STEP 3


New Backup Job
Processing Mode
Choose how VM virtual disk images should be retrieved from storage during backup.
Direct SAN access
VM data is retrieved using vStorage API directly from SAN. This mode requires that Veeam Backup server is connected directly into SAN fabric, otherwise VM processing will fail.
Virtual Appliance
VM data is retrieved from the shared storage through ESX I/O stack. This mode can only be used if Veeam Backup is installed in a VM. Refer to product's documentation for additional requirements.
Network
VM data is retrieved using vStorage API through ESX host over LAN using the NBD (Network Block Device) protocol.
Click Advanced to customize failover and encryption settings.
Advanced
< Back
Next >
Cancel

Select **Direct SAN access**.

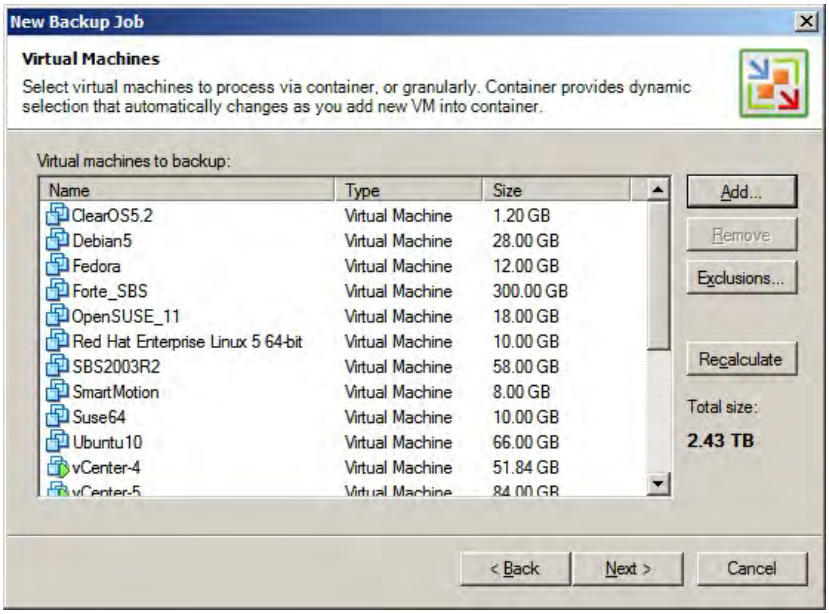
NOTE: Veeam Backup & Replication version 5 fails back to Network mode if SAN mode fails or is not configured correctly on the backup server, which could affect the performance of backups.

STEP 4



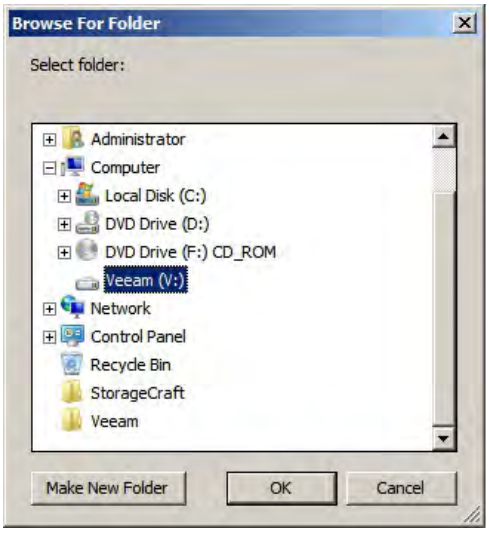
Select the VMs to be backed up.

STEP 5


New Backup Job
Virtual Machines
Select virtual machines to process via container, or granularly. Container provides dynamic selection that automatically changes as you add new VM into container.
Virtual machines to backup:
Name
Type
Size
ClearOS5.2 Virtual Machine 1.20 GB
Debian5 Virtual Machine 28.00 GB
Fedora Virtual Machine 12.00 GB
Forte_SBS Virtual Machine 300.00 GB
OpenSUSE_11 Virtual Machine 18.00 GB
Red Hat Enterprise Linux 5 64-bit Virtual Machine 10.00 GB
SBS2003R2 Virtual Machine 58.00 GB
SmartMotion Virtual Machine 8.00 GB
Suse64 Virtual Machine 10.00 GB
Ubuntu10 Virtual Machine 66.00 GB
vCenter-4 Virtual Machine 51.84 GB
Add...
Remove
Exclusions...
Recalculate
Total size:
2.43 TB
< Back
Next >
Cancel

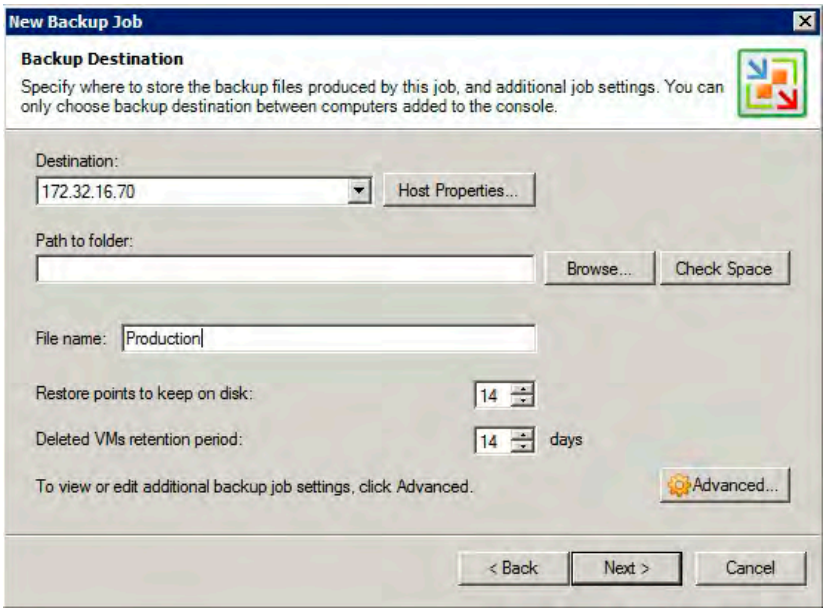
Verify the selected VMs to be backed up and click **Next**.

STEP 6



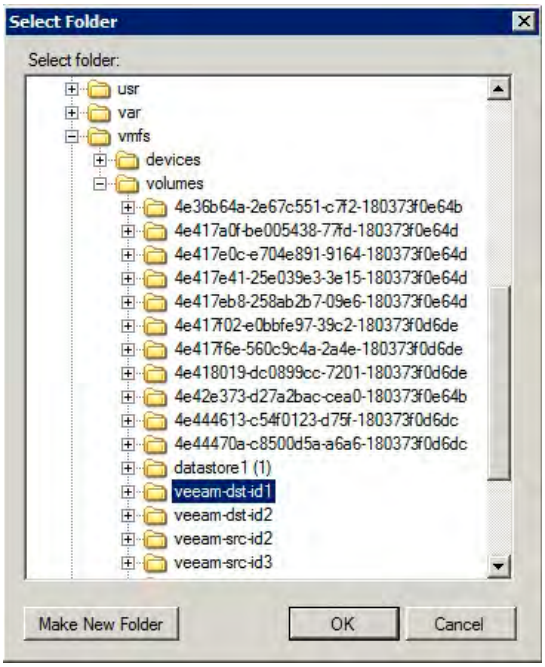
Select a target on which to store backups.

OPTIONAL FOR STEP 6



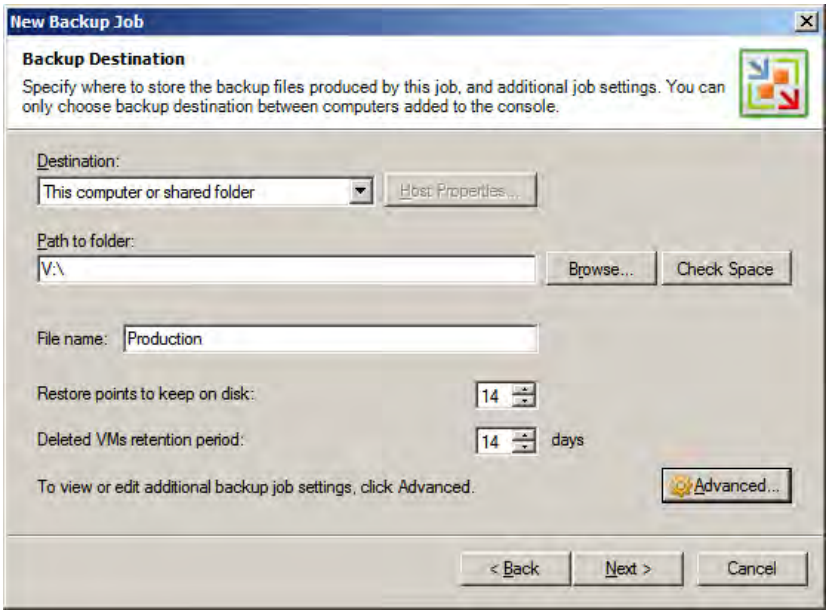
Veeam also allows backups to be stored on a VMFS datastore when leveraging an ESX host, which is not the case for ESXi hosts. With an ESX host, you can opt to select these datastores/volumes as the target. *Note that this configuration may impact performance.*

In this case, the host destination is now an ESX host that holds the VMFS datastores.



Click **Browse** to locate the datastore and click **OK**.

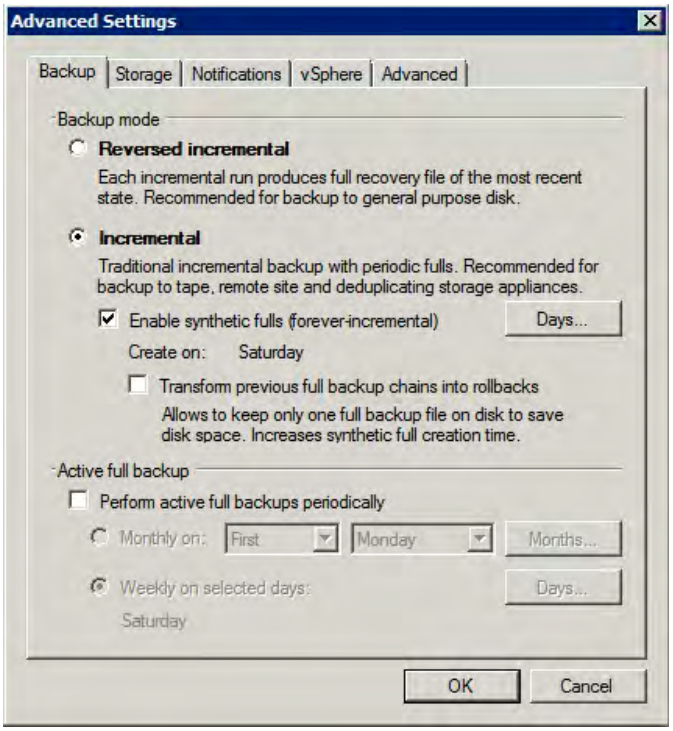
STEP 7



Selecting a VMFS datastore as the destination for backups can have a significant decrease in performance. So in this example, the local disk/iSCSI volume (V:\) is used instead of the default.

Verify that this information is correct and click **Advanced**.

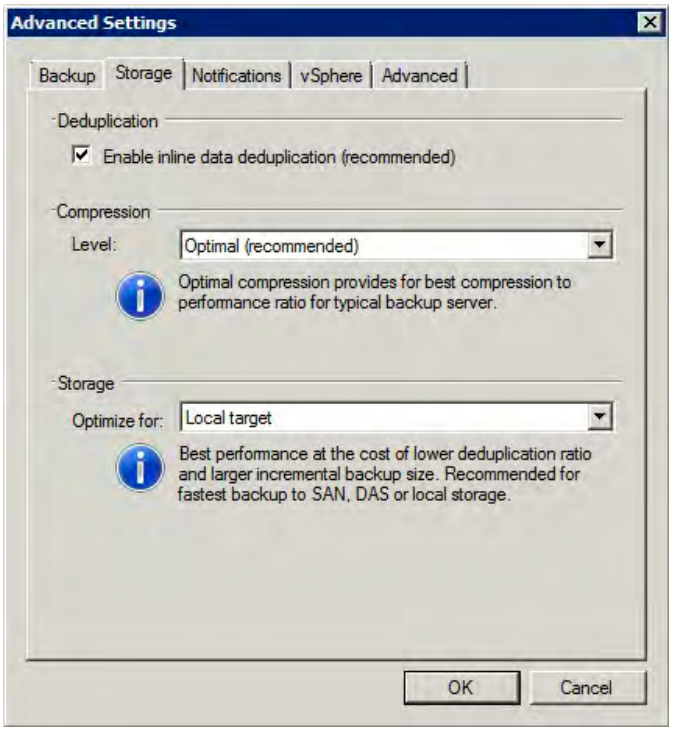
STEP 8



Select the **Incremental** backup mode.

In addition to incremental backups, active full backups should be performed either weekly or monthly. Select the option that works best in your environment.

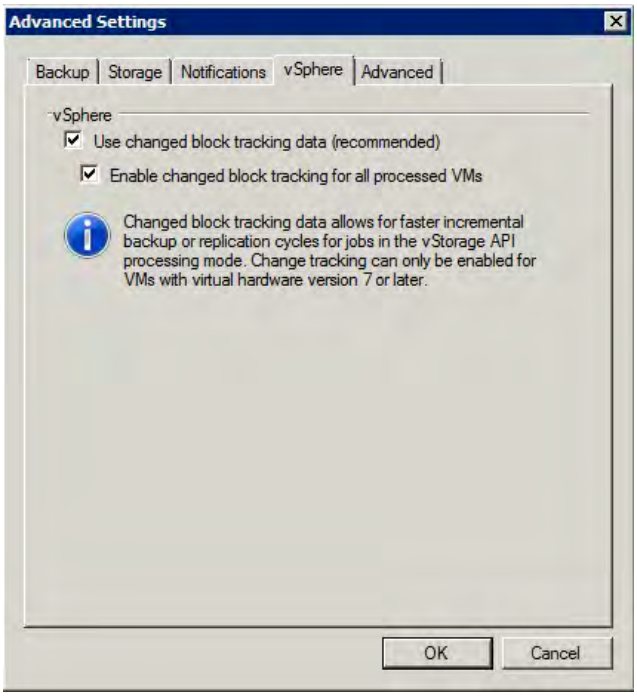
STEP 9



Click the **Storage** tab.

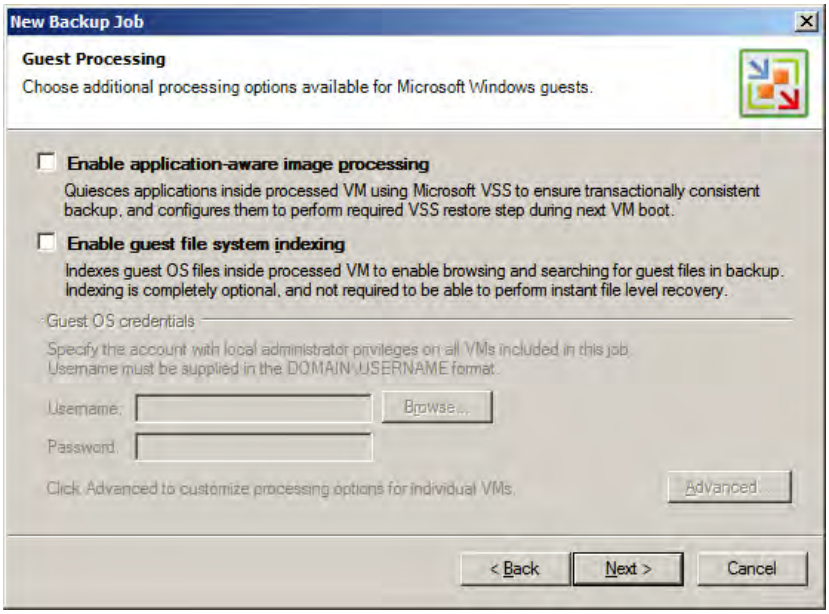
If you wish, enable "Inline data deduplication." Make sure that compression is set to **Optimal** and that it is optimized for **Local target**.

STEP 10


Advanced Settings
Backup
Storage
Notifications
vSphere
Advanced
vSphere
Use changed block tracking data (recommended)
Enable changed block tracking for all processed VMs
Changed block tracking data allows for faster incremental backup or replication cycles for jobs in the vStorage API processing mode. Change tracking can only be enabled for VMs with virtual hardware version 7 or later.
OK
Cancel

Click the **vSphere** tab and select "Use changed block tracking data."

STEP 11

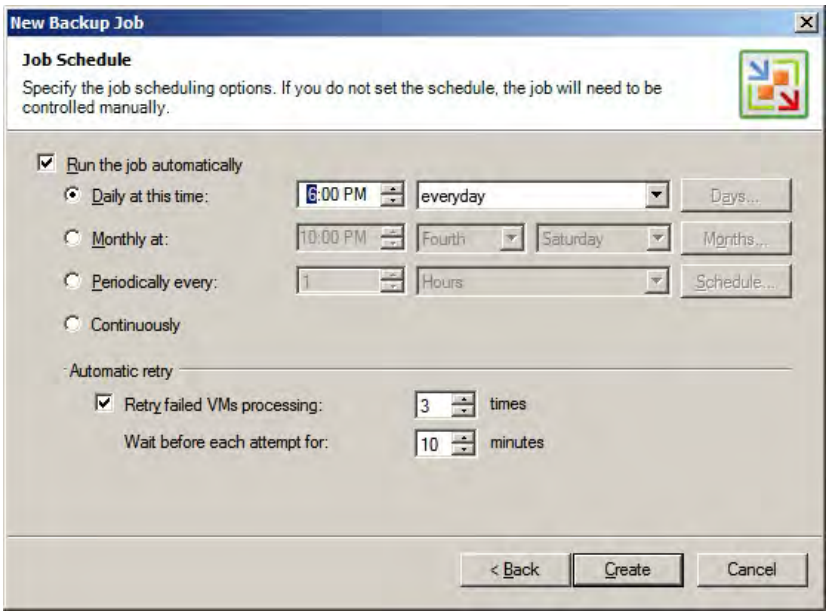

New Backup Job
Guest Processing
Choose additional processing options available for Microsoft Windows guests.
Enable application-aware image processing
Quiesces applications inside processed VM using Microsoft VSS to ensure transactionally consistent backup, and configures them to perform required VSS restore step during next VM boot.
Enable guest file system indexing
Indexes guest OS files inside processed VM to enable browsing and searching for guest files in backup. Indexing is completely optional, and not required to be able to perform instant file level recovery.
Guest OS credentials
Specify the account with local administrator privileges on all VMs included in this job. Username must be supplied in the DOMAIN\USERNAME format.
Username:
Browse...
Password:
Click Advanced to customize processing options for individual VMs.
Advanced...
< Back
Next >
Cancel

Choose additional options for Windows guests.

If you enable either of the additional options, provide a local administrator login.

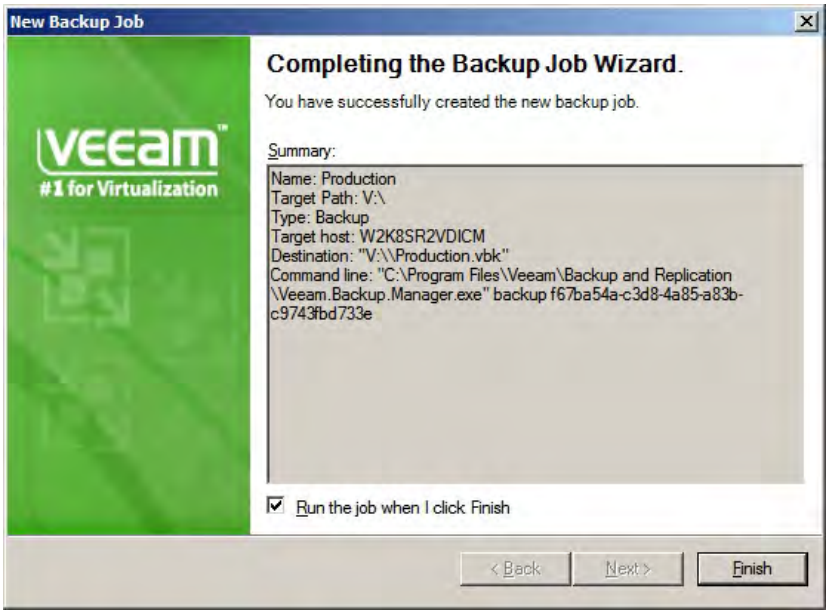
For more information on application processing and Volume Shadow Copy Services, refer to the Veeam Backup & Replication User Guide at: http://www.veeam.com/vmware-esx-backup/resources.html.

STEP 12

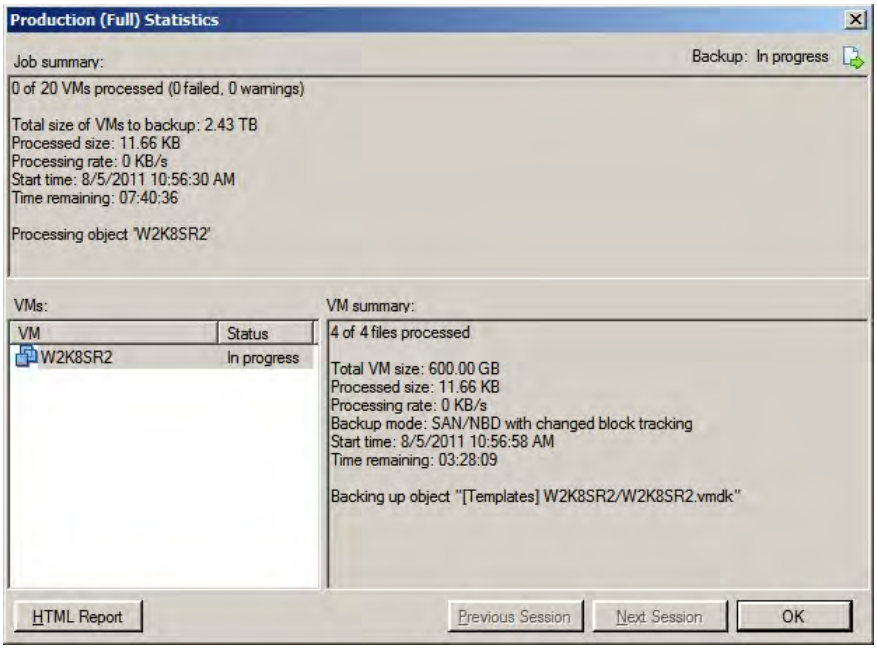


Specify scheduling options.

STEP 13



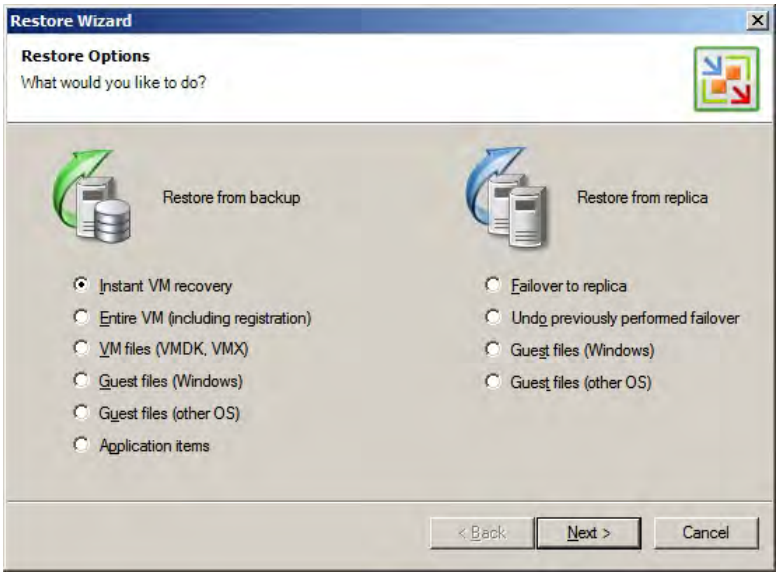
Click **Finish** to complete the Backup Job wizard.



This is an example of real-time statistics for a backup job in progress.

Restoring Virtual Machines with Veeam Backup

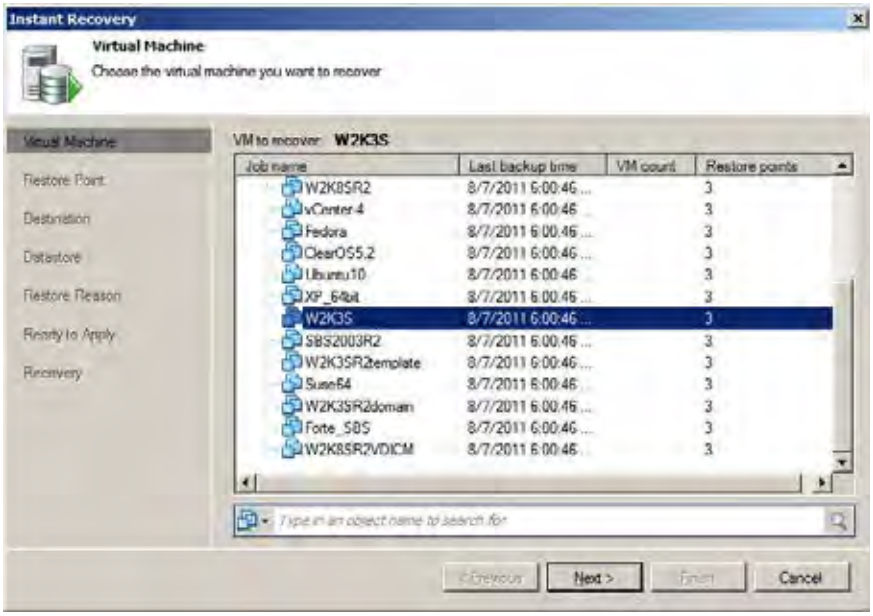
STEP 1



Select the **Restore from Backup** option in the Veeam main console. A wizard guides you through the configuration.

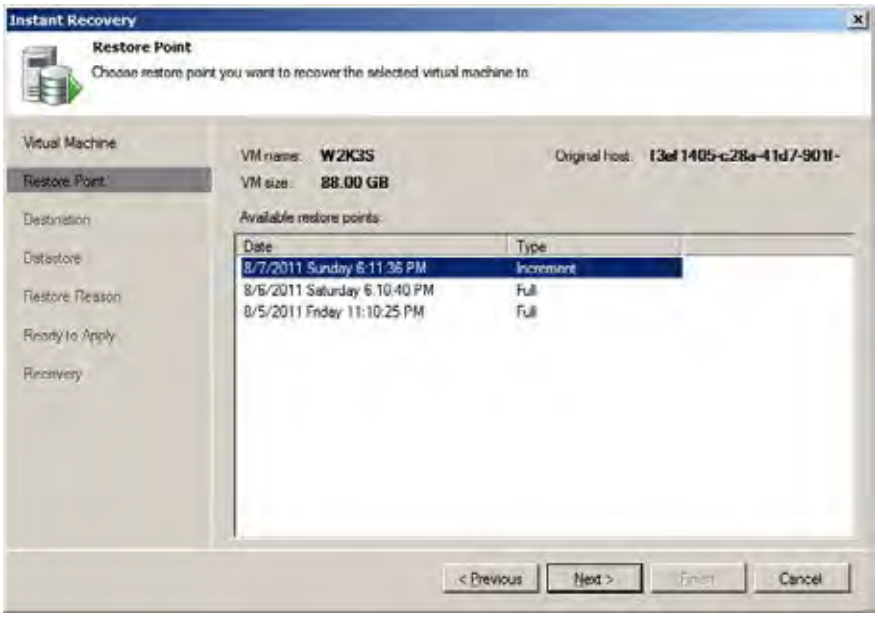
In this example "Instant VM recovery" was selected as a restore point.

STEP 2



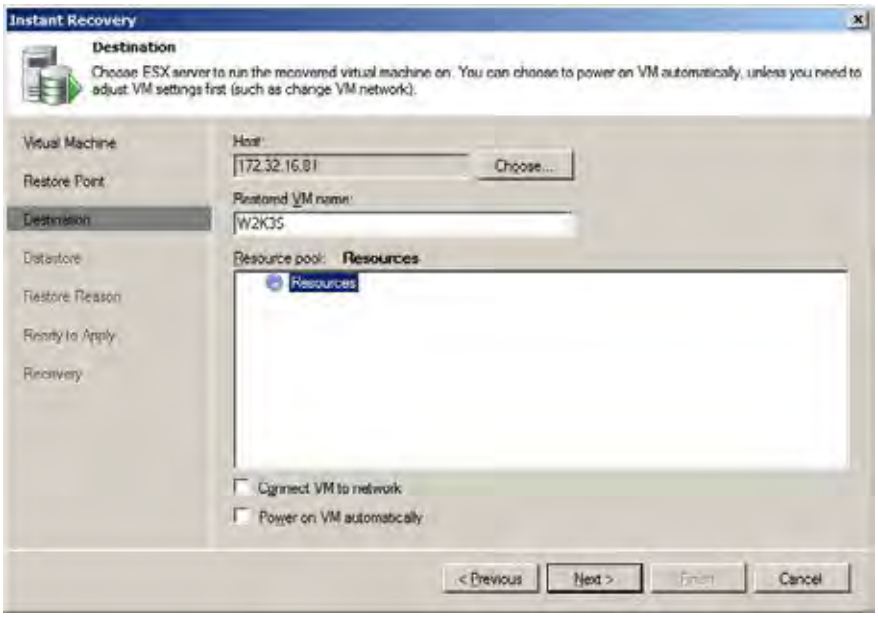
Chose the VM you want to restore.

STEP 3



Choose a restore point.

STEP 4



Choose which vSphere server to restore to.

Copyright 2011 Drobo, Inc. Data Robotics, Drobo, DroboEllite, DroboPro, BeyondRAID, and Smart Volumes are trademarks of Drobo, Inc., which may be registered in some jurisdictions. All other trademarks used are owned by their respective owners. All rights reserved. Specifications subject to change without notice. • HT-0044-00 • August 2011